

# Configure the Merge of Management and Diagnostic Interface in FMC

## Contents

---

[Introduction](#)

[Prerequisites](#)

[Background information](#)

[Components Used](#)

[Configure](#)

[FTD Internal Architecture Diagram](#)

[Convergence Procedure](#)

[Verify](#)

[Troubleshoot - Study Case](#)

[Before Convergence Configuration](#)

[After Convergence Configuration](#)

---

## Introduction

This document describes the steps to configure the merge of the management and diagnostic interfaces, feature added in FTD 7.4.0 version release.

## Prerequisites

Cisco recommended you have knowledge on these topics:

- Cisco Secure Firewall Threat Defense (FTD)
- Cisco Secure Firewall Manager Center (FMC)

## Background information

In Version 7.3 and earlier, the physical management interface is shared between the Diagnostic logical interface (Lina) and the Management logical interface (Linux).

In Version 7.4 and later, the Diagnostic interface is merged with Management for a simplified user experience.

For new devices using 7.4 and later, you cannot use the legacy Diagnostic interface. Only the merged Management interface is available.

## Components Used

The information in this document is based on these software and hardware versions:

- Virtual Cisco Secure Firewall Threat Defense (FTD), version 7.4.2

- Virtual Cisco Secure Firewall Manager Center (FMC), version 7.4.2

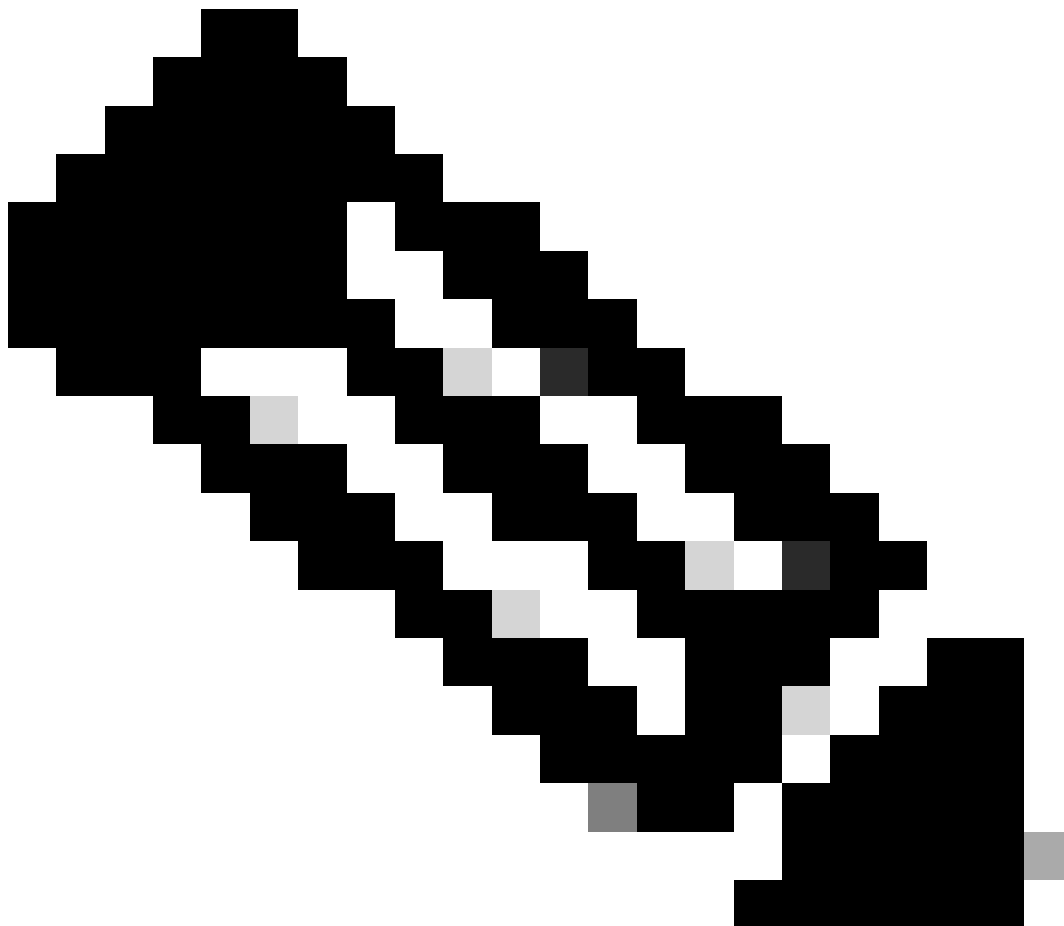
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

## Configure

If you upgraded to 7.4 or later, and you have configuration for the Diagnostic interface, then you have the choice to merge the interfaces manually, or you can continue to use the separate Diagnostic interface.

In case you did not have any configuration for the Diagnostic interface, the interfaces merge is done automatically.

---

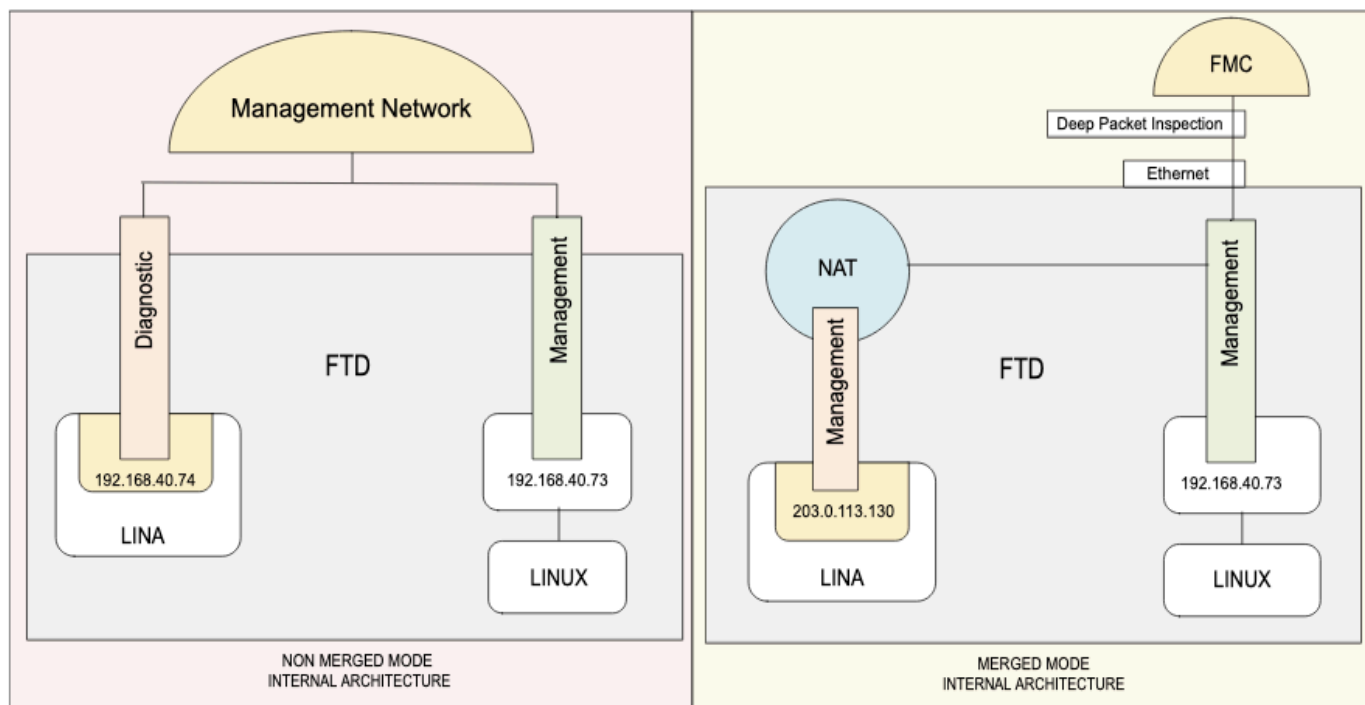


**Note:** Support for the Diagnostic interface is to be removed in a later release, therefore, plan to merge the interfaces as soon as possible.

---

# FTD Internal Architecture Diagram

## Converged Management Interface Overview



*Overview of the Internal Architecture before and after Convergence Management Interface*

On the left, the internal architecture for Diagnostic logical interface (Lina) and the Management logical interface (Linux). Version 7.3 and earlier.

On the right, the internal architecture for a single Management interface. Lina access to the management network uses the NAT service.

## Convergence Procedure

In the case where configuration exists in the Diagnostic interface, the interfaces are not merged automatically after an upgrade, and you need to perform the convergence procedure.

This procedure requires you to acknowledge configuration changes, and in some cases, manually fix the configuration.

To view the current mode of the device, enter the show management-interface converge command at the FTD CLI Clish

```
> show management-interface convergence
no management-interface convergence
```

That result shows that the Management interfaces are not merged.

### Step 1.

On the FMC UI, navigate to **Devices > Device Management**, and select the FTD to be edit. It opens directly to the **Interfaces** tab.

Firewall Management Center  
Devices / Secure Firewall Interfaces

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 10 ⚙️ ? admin ✓ **SECURE**

### Tac\_test

Cisco Firepower Threat Defense for VMware

Device Interfaces **Inline Sets** Routing DHCP VTEP

Management Interface action needed.

Merge the Management and Diagnostic interfaces on the [Management Interface Merge](#) dialog box, or merge them later by clicking the ➤ icon for Diagnostic interface in the table below. Merging the interface will cause some downtime. [Learn more](#)

All Interfaces Virtual Tunnels 🔍 Search by name Sync Device Add Interfaces ▼

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router	
Diagnostic0/0	diagnostic	Physical			192.168.40.74/255.255.255.0(Stat...	Disabled	Global	✎ ➤
GigabitEthernet0/0		Physical				Disabled		✎
GigabitEthernet0/1		Physical				Disabled		✎
GigabitEthernet0/2		Physical				Disabled		✎

Action needed to merge Diagnostic and Management Interface after device upgrade to software version 7.4.2

## Step 2.

Remove all configuration on the Diagnostic interface. It is mandatory that the Diagnostic interface do not have any configuration to continue with the merge.

For example, in this Diagnostic interface, there is: IP address and Static route.

Firewall Management Center  
Devices / Secure Firewall Interfaces

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 10 ⚙️ ? admin ✓ **SECURE**

### Tac\_test

Cisco Firepower Threat Defense for VM

Device Interfaces **Inline Sets**

Management Interface action

Merge the Management and Diagnostic

Merging the interface will cause some d

All Interfaces Virtual Tunnels 🔍 Search by name Sync Device Add Interfaces ▼

Interface

- Diagnostic0/0
- GigabitEthernet0/0
- GigabitEthernet0/1
- GigabitEthernet0/2

Edit Physical Interface

General **IPv4** IPv6 Path Monitoring Hardware Configuration Manager Access Advanced

IP Type:  
Use Static IP ▼

IP Address:  
192.168.40.74/255.255.255.0

eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

Cancel OK

Remove Diagnostic interface IP address

Firewall Management Center  
Devices / Secure Firewall Routing

Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 ⚙️ ? admin ✓ CISCO SECURE

### Tac\_test

Cisco Firepower Threat Defense for VMware

Device Interfaces Inline Sets **Routing** DHCP VTEP

Manage Virtual Routers

Global ▾

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EIGRP

RIP

Policy Based Routing

▼ BGP

    IPv4

    IPv6

Static Route

▼ Multicast Routing

+ Add Route

Network ▲	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked	
▼ IPv4 Routes							
DNS	diagnostic	Global	192.168.40.254	false	1		
▼ IPv6 Routes							

Static Route configure on Diagnostic interface

### Step 3.

Click on the **Management Interface Merge** action needed area or the **Merge icon** next to Edit icon (pencil) on the Diagnostic interface.

Firewall Management Center  
Devices / Secure Firewall Interfaces

Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 ⚙️ ? admin ✓ CISCO SECURE

### Tac\_test

Cisco Firepower Threat Defense for VMware

Device **Interfaces** Inline Sets Routing DHCP

Management Interface action needed.

Merge the Management and Diagnostic interfaces on the Management interface. Merging the interface will cause some downtime. [Learn more](#)

All Interfaces Virtual Tunnels

Interface	Logical Name
Diagnostic0/0	diagnostic
GigabitEthernet0/0	
GigabitEthernet0/1	
GigabitEthernet0/2	

#### Management Interface Merge

- The management interface merge will be synced to the standby/data unit. The IP addresses shown in the "Review Uses" section shows the active unit's active address.
- After you click Proceed, IP address changes will be saved, and you cannot revert the management interface merge, even if you discard the deployment.
- Diagnostic interface static routing is no longer supported; you must delete the route before you can proceed. [Learn more](#)
- HA monitoring for diagnostic interface is not supported.

In this release, you can merge the Management and Diagnostic interfaces to use the single IP instead of two IP addresses. The merged interface will be called Management and use the current management IP address. You will need to update all external services that communicate with Diagnostic IP address. [Learn more](#)

Proceed Cancel

Sync Device Add Interfaces ▾

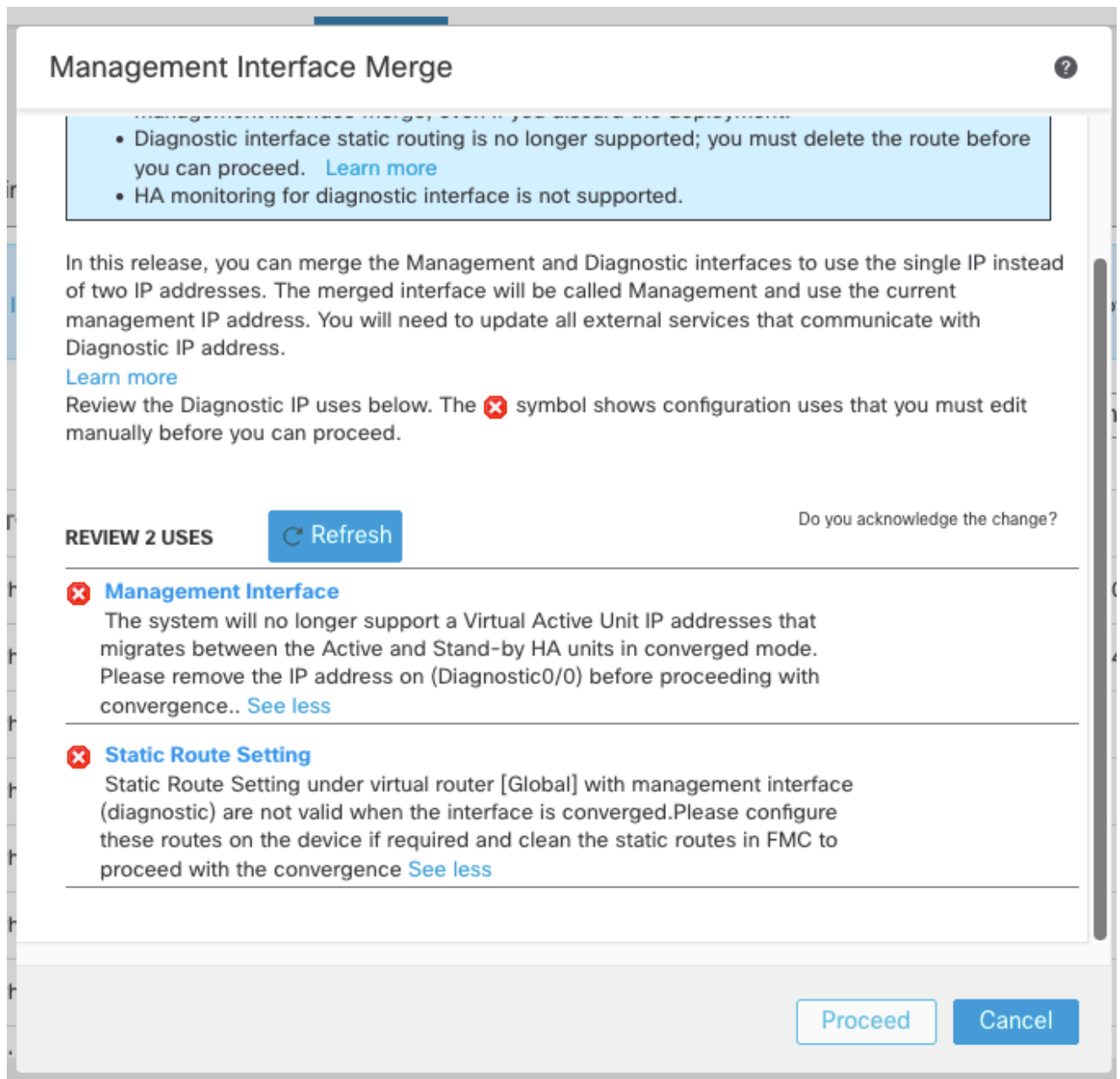
Path Monitoring	Virtual Router	
Disabled	Global	
Disabled		
Disabled		
Disabled		

Management Interface Merge information before proceed



**Note:** For High Availability pairs and clusters, perform this task on the active/control unit. The merged configuration is replicated automatically to the standby/data units.

- 
- For any occurrence that requires to be manual change or removal, a warning icon can appear.



*Example of warning about configurations needed to be removed before merge*

If that is the case: cancel the dialog box, proceed with the removal of the configuration or reconfiguration, and then reopen the Management Interface Merge dialog box.

- Platform Settings that are going to work on the device are marked with a caution icon and require acknowledgement.


## Management Interface Merge

? x

- The management interface merge will be synced to the standby unit. The IP addresses shown in the "Review Uses" section shows the active unit's active address.
- After you click Proceed, IP address changes will be saved, and you cannot revert the management interface merge, even if you discard the deployment.
- Diagnostic interface static routing is no longer supported; you must delete the route before you can proceed. [Learn more](#)
- HA monitoring for diagnostic interface is not supported.

In this release, you can merge the Management and Diagnostic interfaces to use the single IP instead of two IP addresses. The merged interface will be called Management and use the current management IP address. You will need to update all external services that communicate with Diagnostic IP address.

[Learn more](#)

Review the Diagnostic IP uses below. The  symbol shows configuration uses that you must edit manually before you can proceed.

REVIEW 2 USES

 Refresh

Do you acknowledge the change?

### HTTP Access

Management interface (management) is used in (HTTP Access) of PF... [See more](#)



### ICMP Access

Management interface (management) is used in (ICMP Access) of PF... [See more](#)



Cancel

Proceed

*Example of warning of Platform Settings configurations that must be edited*

- Click the box in **Do you acknowledge the change?** column, and then click **Proceed**.

### Step 4.

After the configuration is merged, a banner of success is shown:

*"The Management interface merge was saved and is ready to be deployed.*

*Note that you cannot undo the configuration changes related to merge; you must manually reconfigure the Diagnostic interface and related configuration."*



Deploy the the new merged configuration.

Management interface merge is saved and ready to be deployed

The Management interface is shown on the Interfaces page, although it is read-only.

After deployment, the convergence procedure on Management interface is complete.

### Step 5. Optional

If you had any external services that communicated with the Diagnostic interface, you need to change their configuration to use the Management interface IP address, as the Management Route fallback has been removed on converged mode.

For example:

- SNMP client
- RADIUS server
- DNS server to be reachable via the management network, the user must explicitly select “**Enable DNS Lookup via diagnostic/Management Interface also.**” on **Platform Settings > DNS configuration** as an exception is set for DNS lookups and ICMP (ping and traceroute): in these cases, the threat defense uses data and then fall back to management automatically if a route is not found.

The use of static routes for management interface can only be configured via the FTD CLI Clish (Linux)

Lina management port default route sends all frames to the Linux module.

```
> configure network static-routes ipv4 add management ?  
IP address AAA.BBB.CCC.DDD where each part is in the range 0-255 destination address
```

On the FMC UI, the Management interface is grayed out for selection.

**Add Static Route Configuration**

Type: ☒ IPv4 ☐ IPv6

Interface\*

Null0 (indicates it is available for route leak)

management

Search

management  
This interface is not useable in Converged mode.

Selected Network

10.151.103.167  
10.151.110.13  
10.151.110.14  
10.151.110.15  
10.151.110.16  
10.151.113.35

< Viewing 1-100 of 3660 >

*Management interface is not available for selection on static routes after merge is complete.*

## Verify

Expected changes after merge on the Management Interface

- Verify the convergence mode on FTD CLI Clish by executing command

```
> show management-interface convergence
management-interface convergence
```

- On FMC UI, the Interface name is changed to Management0/0 , Logical name to management.

Firewall Management Center  
Devices / Secure Firewall Interfaces

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ? admin ✓ CISCO SECURE

**Tac\_test** Save Cancel

Cisco Firepower Threat Defense for VMware

Device **Interfaces** Inline Sets Routing DHCP VTEP

All Interfaces Virtual Tunnels 🔍 Search by name Sync Device Add Interfaces ▼

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router	
Management0/0	management	Physical				Disabled	Global	🔍 ↺
GigabitEthernet0/0		Physical				Disabled		✎
GigabitEthernet0/1		Physical				Disabled		✎
GigabitEthernet0/2		Physical				Disabled		✎

*Merge confirmation on Management Interface name and Logical name*

- On FTD CLI Clish, the new IP addresses are automatically configured on Lina for Management interface.  
NAT is used as an internal implementation: The internal private IPv4 address 203.0.113.130 and IPv6 address fd00:0:1:1::2 are the ones assigned (both subject to change).  
Those IPs are NATed to the public Linux Kernel FTD IPv4 and IPv6 addresses, therefore there is no need for public IPs on Lina anymore.

In expert mode, “ifconfig” displays Internal IPv4 (203.0.113.129) and IPv6 (fd00:0:1:1::1) address for Linux.

FTD CLI Clish:

```
> show interface management
Interface Management0/0 "management", is up, line protocol is up
  Hardware is en_vtun rev00, DLY 10 usec
    Input flow control is unsupported, output flow control is unsupported
    MAC address 0050.56b3.f75d, MTU 1500
    IP address 203.0.113.130, subnet mask 255.255.255.248
```

Expert mode on Linux:

```
root@ftd01:/home/admin# ifconfig
...
tap5: flags=4419<UP,BROADCAST,RUNNING,PROMISC,MULTICAST> mtu 1500
    inet 203.0.113.129 netmask 255.255.255.248 broadcast 203.0.113.135
    inet6 fe80::8403:9ff:fe6b:6d16 prefixlen 64 scopeid 0x20<link>
    inet6 fd00:0:1:1::1 prefixlen 123 scopeid 0x0<global>
```

## Troubleshoot - Study Case

In this study case, the Diagnostic interface on a virtual FTD has configured a separate IP addresses for connectivity to external services of DNS Lookup, before upgrade to 7.4.2.

After the upgrade to 7.4.2, the convergence is needed, this is how the configuration in the FMC UI, FTD CLI Lina and Linux is, before and after the merge.

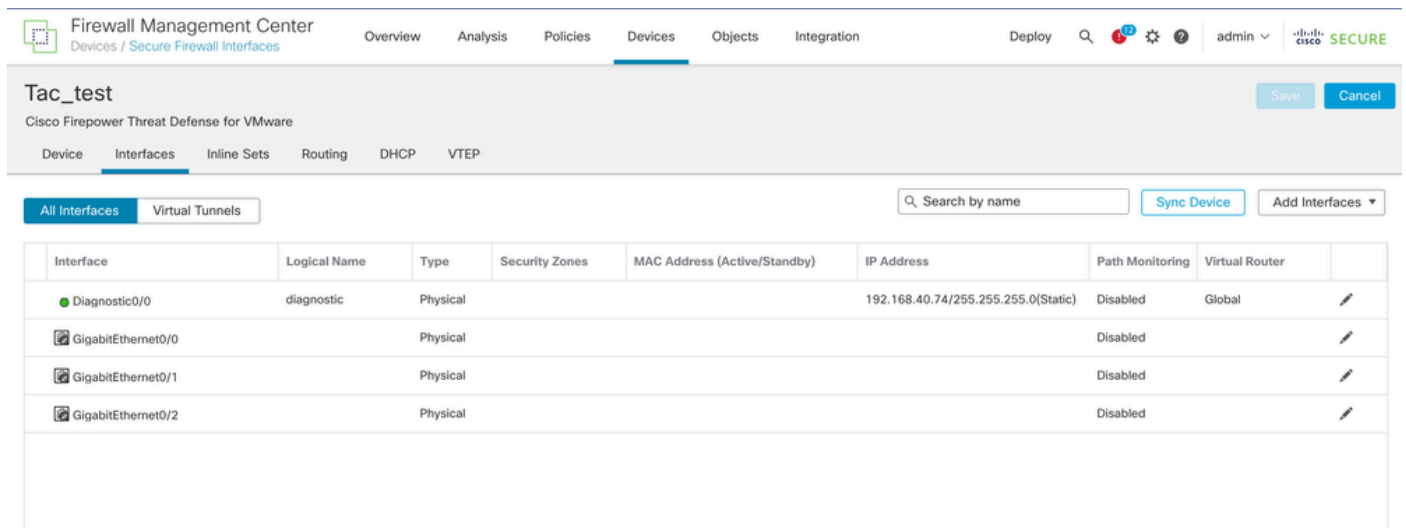
There are also traffic captures on FTD CLI Lina and Linux to show the traffic using the logical Diagnostic

interface move to use the Management interface.

## Before Convergence Configuration

The Diagnostic interface has a separate IP and a static route for the DNS Lookup, this way it works using both logical interfaces from Lina to Linux in the FTD.

### FMC UI Configuration



Firewall Management Center  
Devices / Secure Firewall Interfaces

Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 12 ⚙️ ⓘ admin ▾ CISCO SECURE

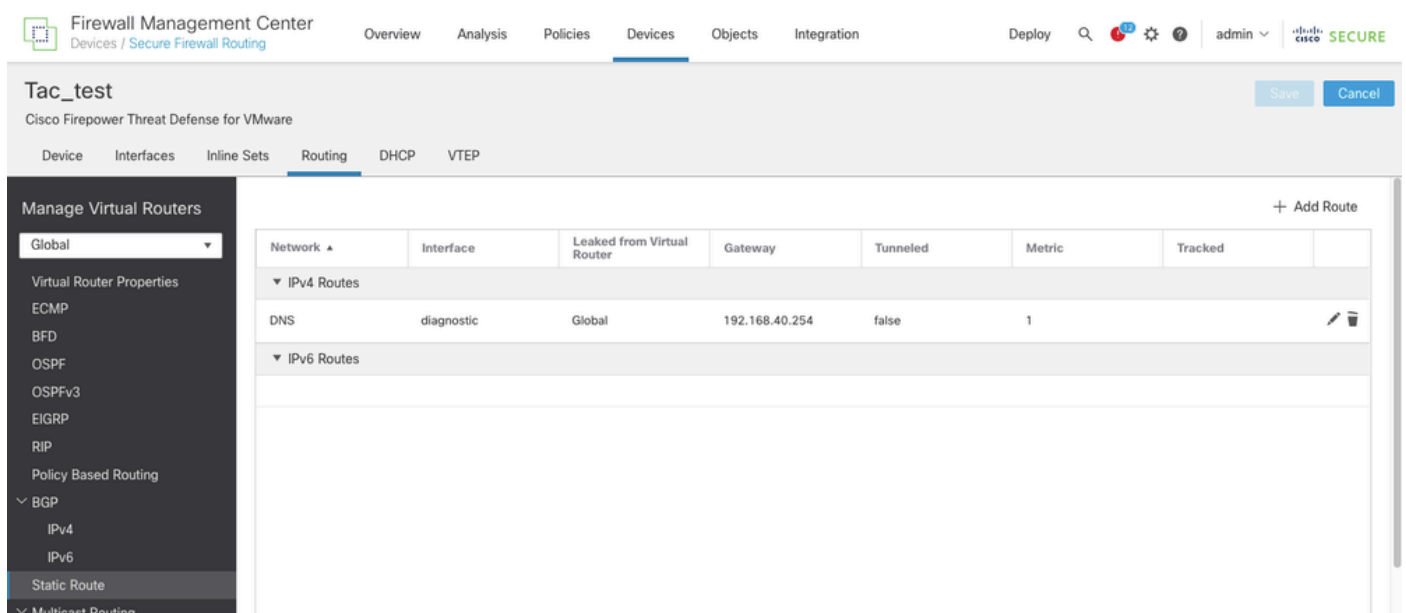
**Tac\_test** Cisco Firepower Threat Defense for VMware [Save] [Cancel]

Device **Interfaces** Inline Sets Routing DHCP VTEP

All Interfaces Virtual Tunnels 🔍 Search by name [Sync Device] [Add Interfaces ▾]

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router	
Diagnostic0/0	diagnostic	Physical			192.168.40.74/255.255.255.0(Static)	Disabled	Global	✎
GigabitEthernet0/0		Physical				Disabled		✎
GigabitEthernet0/1		Physical				Disabled		✎
GigabitEthernet0/2		Physical				Disabled		✎

*Diagnostic interface configuration before merge*



Firewall Management Center  
Devices / Secure Firewall Routing

Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 12 ⚙️ ⓘ admin ▾ CISCO SECURE

**Tac\_test** Cisco Firepower Threat Defense for VMware [Save] [Cancel]

Device Interfaces Inline Sets **Routing** DHCP VTEP

Manage Virtual Routers  
Global ▾  
Virtual Router Properties  
ECMP  
BFD  
OSPF  
OSPFv3  
EIGRP  
RIP  
Policy Based Routing  
BGP  
IPv4  
IPv6  
Static Route  
Multicast Routing

+ Add Route

Network ▲	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked	
▼ IPv4 Routes							
DNS	diagnostic	Global	192.168.40.254	false	1		✎ 🗑
▼ IPv6 Routes							

*Static Route configured on Diagnostic interface*

DNS configuration over

**Devices > Platform Settings**, select the policy, then **DNS** tab.



## FQDN\_Test\_PlatformSettings

Enter Description

ARP Inspection

Banner

DNS

External Authentication

Fragment Settings

HTTP Access

ICMP Access

NetFlow

SSH Access

SMTP Server

SNMP

SSL

Syslog

Timeouts

Time Synchronization

Time Zone

UCAPL/CC Compliance

Performance Profile

DNS Settings

Trusted DNS Servers

### DNS Resolution Settings

Specify DNS servers group and device interfaces to reach them.

☒ Enable DNS name resolution by device

DNS Server Groups

Add

**DNS\_Server\_lab** (Default)  
any



Expiry Entry Timer:

1

Range: 1-65535 minutes

Poll Timer:

240

Range: 1-65535 minutes

DNS configuration in Platform Settings

# FQDN\_Test\_PlatformSettings

Enter Description

ARP Inspection

Banner

DNS

External Authentication

Fragment Settings

HTTP Access

ICMP Access

NetFlow

SSH Access

SMTP Server

SNMP

SSL

Syslog

Timeouts

Time Synchronization

Time Zone

UCAPL/CC Compliance

Performance Profile

1

Range: 1-65535 minutes

Poll Timer:

240

Range: 1-65535 minutes

## Interface Objects

Devices will use specified interface objects for connecting with DNS Servers.

Available Interface Objects

Q Search

Selected Interface Objects

Add



Enable DNS Lookup via diagnostic/Management interface also.

Check box selected for Enable DNS Lookup via diagnostic/Management interface also

## Configuration for Diagnostic Interface over FTD Lina

```
interface Management0/0
management-only
nameif diagnostic
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 192.168.40.74 255.255.255.0
```

ftd01# sh ip

System IP Addresses:

Interface	Name	IP address	Subnet mask	Method
Management0/0	diagnostic	192.168.40.74	255.255.255.0	manual

Current IP Addresses:

Interface	Name	IP address	Subnet mask	Method
Management0/0	diagnostic	192.168.40.74	255.255.255.0	manual

ftd01# sh route management-only

Routing Table: mgmt-only

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
 E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN  
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2  
 ia - IS-IS inter area, \* - candidate default, U - per-user static route  
 o - ODR, P - periodic downloaded static route, + - replicated route  
 SI - Static InterVRF, BI - BGP InterVRF

Gateway of last resort is not set

```

S      10.10.10.10 255.255.255.255 [1/0] via 192.168.40.254, diagnostic
C      192.168.40.0 255.255.255.0 is directly connected, diagnostic
L      192.168.40.74 255.255.255.255 is directly connected, diagnostic
  
```

## DNS configuration on FTD CLI Lina

```

ftd01# sh run dns
dns domain-lookup diagnostic
DNS server-group DNS_Server_lab
    retries 5
    timeout 15
    name-server 10.10.10.10 diagnostic
    domain-name test.lab
DNS server-group DefaultDNS
dns-group DNS_Server_lab
  
```

## Capture on the diagnostic interface for DNS traffic going to the DNS server 10.10.10.10

```

ftd01# sh cap
capture diag type raw-data trace detail interface diagnostic [Capturing - 340 bytes]
    match udp any host 10.10.10.10 eq domain
  
```

```
ftd01# sh cap diag
```

5 packets captured

```

1: 00:15:39.660442      192.168.40.74.59939 > 10.10.10.10.53:  udp 27
2: 00:15:54.661953      192.168.40.74.59939 > 10.10.10.10.53:  udp 27
3: 00:16:09.661739      192.168.40.74.59939 > 10.10.10.10.53:  udp 27
4: 00:16:24.667674      192.168.40.74.59939 > 10.10.10.10.53:  udp 27
5: 00:16:39.684946      192.168.40.74.59939 > 10.10.10.10.53:  udp 27
  
```

5 packets shown

```
ftd01#
```

## Capture on Linux expert mode, to confirm the correct flow of the DNS Lookup traffic on the Management interface from the Diagnostic interface

```

root@ftd01:/home/admin# tcpdump -i br1 port 53
HS_PACKET_BUFFER_SIZE is set to 4.
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on br1, link-type EN10MB (Ethernet), capture size 262144 bytes
  
```

```

04:58:14.648941 IP 192.168.40.74.49171 > 10.10.10.10.domain: 5655+ AAAA? cisco.com. (27)
04:58:29.656317 IP 192.168.40.74.11606 > 10.10.10.10.domain: 26905+ A? cisco.com. (27)
04:58:44.686568 IP 192.168.40.74.11606 > 10.10.10.10.domain: 24324+ A? cisco.com. (27)
04:58:59.704586 IP 192.168.40.74.11606 > 10.10.10.10.domain: 35592+ A? cisco.com. (27)
04:59:14.742685 IP 192.168.40.74.11606 > 10.10.10.10.domain: 40993+ A? cisco.com. (27)
04:59:29.763690 IP 192.168.40.74.11606 > 10.10.10.10.domain: 62225+ A? cisco.com. (27)
04:59:44.796484 IP 192.168.40.74.11606 > 10.10.10.10.domain: 25350+ A? cisco.com. (27)

```

## After Convergence Configuration

As mention on the convergence procedure, in order to do the merge, all configurations on the Diagnostic Interface must be removed.

These is the information on FMC and FTD CLI once the Merge is complete.

Management Interface configuration over FMC UI

**Devices > Device Management**, select the FTD. It opens directly to the **Interfaces** tab.

The screenshot shows the FMC interface for a device named 'Tac\_test'. The 'Interfaces' tab is selected, displaying a table of network interfaces. The table has columns for Interface, Logical Name, Type, Security Zones, MAC Address (Active/Standby), IP Address, Path Monitoring, and Virtual Router. The 'Management0/0' interface is highlighted.

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router
Management0/0	management	Physical				Disabled	Global
GigabitEthernet0/0		Physical				Disabled	
GigabitEthernet0/1		Physical				Disabled	
GigabitEthernet0/2		Physical				Disabled	

*Management Interface after the merge*

The screenshot shows the FMC interface for a device named 'Tac\_test'. The 'Routing' tab is selected, displaying a table of network routes. The table has columns for Network, Interface, Leaked from Virtual Router, Gateway, Tunneled, Metric, and Tracked. The 'Global' virtual router is selected.

Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
IPv4 Routes						
IPv6 Routes						



*No static routes to the DNS server are added*

DNS configuration must remain the same on Platform Settings.

**Devices > Platform Settings**, select the policy, then **DNS** tab.

In order for the DNS Lookup to continue to be sent to the Management Interface without the need to add a static route, the "Enable DNS Lookup via diagnostic/Management interface also." must remain selected.

The screenshot displays the 'Firewall Management Center' interface, specifically the 'Platform Settings Editor' for a policy named 'FQDN\_Test\_PlatformSettings'. The 'Devices' tab is selected in the top navigation bar. On the left, a sidebar lists various settings categories, with 'DNS' highlighted. The main content area is titled 'DNS Resolution Settings' and includes a description: 'Specify DNS servers group and device interfaces to reach them.' A toggle switch for 'Enable DNS name resolution by device' is turned on. Below this, a section for 'DNS Server Groups' features an 'Add' button and a list containing 'DNS\_Server\_lab (Default)' with the interface 'any'. At the bottom, there are two input fields: 'Expiry Entry Timer' set to '1' and 'Poll Timer' set to '240', both with a range of '1-65535 minutes'.

Firewall Management Center  
Devices / Platform Settings Editor

Overview Analysis Policies **Devices** Objects Integration

**FQDN\_Test\_PlatformSettings**  
Enter Description

ARP Inspection  
Banner  
**DNS**  
External Authentication  
Fragment Settings  
HTTP Access  
ICMP Access  
NetFlow  
SSH Access  
SMTP Server  
SNMP  
SSL  
Syslog  
Timeouts  
Time Synchronization  
Time Zone  
UCAPL/CC Compliance  
Performance Profile

**DNS Settings** Trusted DNS Servers

**DNS Resolution Settings**  
Specify DNS servers group and device interfaces to reach them.

☒ Enable DNS name resolution by device

DNS Server Groups **Add**

**DNS\_Server\_lab** (Default)  
any

Expiry Entry Timer:  
 Range: 1-65535 minutes

Poll Timer:  
 Range: 1-65535 minutes

*DNS configuration on Platform Settings*

# FQDN\_Test\_PlatformSettings

Enter Description

ARP Inspection

Banner

DNS

External Authentication

Fragment Settings

HTTP Access

ICMP Access

NetFlow

SSH Access

SMTP Server

SNMP

SSL

Syslog

Timeouts

Time Synchronization

Time Zone

UCAPL/CC Compliance

Performance Profile

1

Range: 1-65535 minutes

Poll Timer:

240

Range: 1-65535 minutes

## Interface Objects

Devices will use specified interface objects for connecting with DNS Servers.

Available Interface Objects

Q Search

Selected Interface Objects

Add



Enable DNS Lookup via diagnostic/Management interface also.

Option for Enable DNS Lookup via diagnostic/Management interface also must remain the same

## Configuration on the FTD CLI

```
> show interface management
```

```
Interface Management0/0 "management", is up, line protocol is up
```

```
Hardware is en_vtun rev00, DLY 10 usec
```

```
Input flow control is unsupported, output flow control is unsupported
```

```
MAC address 0050.56b3.f75d, MTU 1500
```

```
IP address 203.0.113.130, subnet mask 255.255.255.248
```

```
> show interface ip brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	unassigned	YES	unset	administratively down	up
GigabitEthernet0/1	unassigned	YES	unset	administratively down	up
GigabitEthernet0/2	unassigned	YES	unset	administratively down	up
Internal-Control0/0	127.0.1.1	YES	unset	up	up
Internal-Control0/1	unassigned	YES	unset	up	up
Internal-Data0/0	unassigned	YES	unset	down	up
Internal-Data0/0	unassigned	YES	unset	up	up
Internal-Data0/1	169.254.1.1	YES	unset	up	up
Internal-Data0/2	unassigned	YES	unset	up	up
Management0/0	203.0.113.130	YES	unset	up	up

```
ftd01# sh route management-only
```

Routing Table: mgmt-only

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP  
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN  
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2  
ia - IS-IS inter area, \* - candidate default, U - per-user static route  
o - ODR, P - periodic downloaded static route, + - replicated route  
SI - Static InterVRF, BI - BGP InterVRF

Gateway of last resort is not set

## DNS configuration on FTD CLI on LINA side

```
ftd01# sh run dns
dns domain-lookup management
DNS server-group DNS_Server_lab
    retries 5
    timeout 15
    name-server 10.10.10.10 management
    domain-name test.lab
DNS server-group DefaultDNS
dns-group DNS_Server_lab
```

Capture on Linux expert mode, to confirm the correct flow of the DNS Lookup traffic on the Management interface.

```
root@ftd01:/home/admin# tcpdump -i br1 port 53
HS_PACKET_BUFFER_SIZE is set to 4.
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on br1, link-type EN10MB (Ethernet), capture size 262144 bytes
20:20:33.623146 IP ftd01.60310 > 10.10.10.10.domain: 61954+ A? cisco.com. (27)
20:20:33.623533 IP ftd01.33417 > umbrella.domain: 20595+ PTR? 10.10.10.10.in-addr.arpa. (42)
20:20:48.660172 IP ftd01.60310 > 10.10.10.10.domain: 41252+ A? cisco.com. (27)
20:20:52.638426 IP ftd01.39304 > umbrella.domain: 20595+ PTR? 10.10.10.10.in-addr.arpa. (42)
20:21:09.669133 IP ftd01.47150 > umbrella.domain: 39343+ AAAA? ftd01. (23)
20:21:09.669305 IP ftd01.50173 > umbrella.domain: 57694+ AAAA? ftd01. (23)
20:21:11.659352 IP ftd01.48092 > umbrella.domain: 46478+ PTR?.opendns.in-addr.arpa. (45)
20:21:14.673992 IP ftd01.58547 > umbrella.domain: 57694+ AAAA? ftd01. (23)
20:21:18.673371 IP ftd01.47607 > umbrella.domain: 39343+ AAAA? ftd01. (23)
20:21:18.695507 IP ftd01.60310 > 10.10.10.10.domain: 29973+ A? cisco.com. (27)
```

With this evidence, it can be confirmed that the DNS Lookup continue to work even if no static route is added on the Management interface via Linux.